



Spring 2016

Information Security

101

Inside this issue:

Universities top government as most likely Cyber target

Time for an Upgrade: Understanding the IT Lifecycle

Pirated Papers Leaked in Online Publication Hub

Click Here to Win! Free Gift Card for Every Reader!

ARC Program Update: Greenland Deployment Planning

ARC IT Spotlight: Jeffrey Casper, SRI IT & Communications Manager

Universities top government as most likely Cyber target

Imagine you are a hacker picking your next target...will it be a bank, a government agency, or perhaps your alma mater? Whether it's a big payout or government secrets you are after, turns out hacking the academic institution is likely to give you the most bang for your buck! According to Symantec's 2014 Internet Security Threat Report, Academic Institutions topped both government and the financial sector in likelihood of experiencing a cyber incident. In fact, educational institutions ranked third overall in categories of attack, led only by the retail and healthcare sectors in likelihood of experiencing a cyber attack. In one recent example, a 2015 hack against educational giant Penn State compromised servers that contained the personal information of over 18,000 students and faculty, and may have also put confidential Department of Defense engineering research in jeopardy. The attacks appear to have originated from China and were believed to be aimed at aerospace engineering research conducted at the university as part of the institution's partnership with the Pentagon and the U.S. Navy. According to the Wall Street Journal, similar attacks originating from China have occurred in recent years at other major research institutions including Johns Hopkins and MIT. Despite being likely targets, educational institutions are less likely than corporations or government agencies to have appropriate cybersecurity measures in place to protect their assets and information. One industry study found that of a sample of 557

universities, twenty-five percent were vulnerable to a simple Cross-Site Scripting attack. Universities often face tighter Information Security budgets than corporations, and do not always face the same legal requirements for security that protect federal government entities. That means universities are somewhat on their own to implement cybersecurity measures that make sense for their environment. Those efforts are further complicated by students' ability to bring their own devices, and by the high turnover created by the natural cycle of student and faculty populations entering and leaving the university system. Despite the unique challenges they will face, educational institutions must begin to take proper action to protect the personal information of students and faculty as well as the critical research information for which they are responsible. Many consumers already factor cybersecurity into their decision making process when considering an online purchase, and it may soon become more common to consider a university's security posture when deciding where to work, attend school, or award that high stakes research project.

Learn more about the who, when, and how of cyberattacks in Symantec's annual Internet Security Threat Report. The report is publicly available online at: https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf.

Time for an Upgrade: Understanding the IT Lifecycle

Performing scheduled vehicle maintenance, cleaning out the food pantry, upgrading to a new cell phone- nearly everything in life has an expiration date. Sometimes it's out with the old, in with the new as technology paves the way for a better process or device, such as replacing your bulky desktop with a lighter laptop model that boasts more memory in less space. Other times, it's a simple replacement of the same part, like replacing tires on a car. Either way, the ideal goal is to replace an item before it fails so that there is no gap in use. In Information Technology, this concept is known as Lifecycle Management. The goal of Lifecycle Management is to document all assets and their expected life span so that from

the moment a device is deployed, budget and maintenance planning are already underway for its replacement. The driving idea behind Lifecycle Management is that planned outages are easier to manage than unexpected outages. The more a device is relied upon for completion of daily activities, the more important it is that the device be replaced while functioning to avoid an unexpected gap in service. While there are costs incurred by replacing parts that happen to function beyond their normal lifecycle, industry best practice indicates that the productivity savings of avoiding the unplanned outages outweigh the costs of replacing equipment at the end of its expected lifecycle.

Given the unique weather conditions common in the Arctic program, replacing an IT asset before it ever has a chance to fail is also a matter of life and safety. In addition to being a required component of normal security documentation, maintaining detailed hardware and software lists for all offices and sites is important for both IT Contingency Planning and Lifecycle Management. The two are distinct in that Contingency Planning ensures there is a plan in place for unexpected failures, whereas Lifecycle Management plans for the expected failures. Both are necessary for a reliable Information Technology environment, and both are important to Information Security.

Pirated Papers Leaked in Online Publication

After years of effort, the results of most research projects are documented in scientific research papers and made available to the academic community through peer reviewed journals or other members-only institutions. Recently, however, research paper repositories went the way of music file sharing when a Russian hacker exploited member credentials to hundreds of research repositories to post illegally obtained copies of millions of research papers.

Copyright violations to obtain research papers without paying the necessary fees is a common online exploit, but until recently it was typically done on a one-off basis, where an individual requested access to a specific paper and someone who had legitimate access provided a copy. However, the illegal publication site Sci-Hub completely disregards copyright law and boasts access to illegally obtained copies of millions of research papers. Citing what she believes to be an unjust system of charging for access to information, the operator of the site has already defied authorities once by moving the site to an international domain after she was first shut down for violation of copyright law.



Lawsuits based in the United States have limited reach, however, once the site is moved to an international domain or even the “dark net,” a restricted access section of the internet known for illegal file sharing. As public debate continues over whether or not academic research papers should be free and publicly available, millions of papers will remain available online for those who wish to risk visiting the site.

Peer to peer file sharing sites are notorious for creating points of vulnerability on the computers that access them. Visiting the site itself is not advisable given the known security risks of peer sharing sites; however, *The Atlantic* recently published an article that examines the development of SciHub and the complex nature of its legality and continued existence.: <http://www.theatlantic.com/technology/archive/2016/02/the-research-pirates-of-the-dark-web/461829/>.

Click Here to WIN! Free Gift Card for Every Reader!

CLICK HERE TO REDEEM \$25 TO YOUR FAVORITE RESTAURANT! Look familiar? It's springtime, and over the holidays or new year you may have seen a flurry of emails and social media advertisements enticing you to click on a link in order to win a gift card or other reward for your participation. It seems so easy, 'like' a page on Facebook, or enter your email address and a few other personal details and the retailer will reward you for your time with a free gift card. Unfortunately, as you may have suspected, these advertisements are by and large fraudulent. At best, the gift card offer is really a link to a third party data mining company that seeks to sell your email address and contact information to other companies for direct sales. This practice isn't illegal because by clicking on the link and providing your information, you have voluntarily participated. That's frustrating, but at least not harmful. But it's another problem altogether when the gift card link isn't a legitimate company at all and is instead the work of a crafty hacker who is hoping to exploit

your love of a good deal in order to install malware on your computer. Clicking a malicious link is a common way to introduce dangerous files to your machine and may compromise your computer and put you at risk for identity theft.

Facebook scams are

particularly effective at tricking users to your computer and your personal information. Do not click on links from emails, texts, or Facebook unless you can verify they are not malicious. When in doubt, check with the company's customer service group or the Better Business Bureau to determine the validity of a deal that looks too good to be true. It is often difficult to know where the scam originated or who to hold responsible. As the consumer, it's up to you to protect



ARC Program Update: Greenland Deployment Planning

Arctic Sciences Section Information Security Support is provided by SPAWAR Office of Polar Programs

Robert Myer, Program Manager, SPAWAR Office of Polar Programs (SOPP)
843.609.7753
robert.l.myer.civ@mail.mil

Maria Petrie
Arctic Information Security
706.414.1412
petrie_maria@bah.com



Who, Where, & Why?

Each year, the information security team plans an annual deployment to one or more of the field sites supported by the Arctic Sciences Research Support and Logistics Program. One critical benefit of deployment is the opportunity for information security team members to see first-hand how conditions at the Arctic research sites differ from most other sites where federal information security policy is implemented. When providing information security guidance for the program, most experienced professionals will reference the National Institute of Standards and Technology and other federal standards as best practice for establishing a secure computing environment in the Arctic. However, the unique setting of the Arctic sites does not always allow for

implementation of industry standard as would occur at other federal sites. Visiting the sites in-person allows the Information Security team to meet the staff who manage IT assets on a daily basis and gain an understanding of their needs when it comes to IT functionality and IT security. It provides an opportunity to perform hands on assessments of IT assets and networks when necessary, but most importantly, deployments provide context for how Information Technology and Information Security fit into the larger picture of the Arctic research mission.

What is planned for this year's trip?

This year, the Information Security team will venture to Kangerlussuaq and Summit stations. Recent IT network changes at Kangerlussuaq require a security assessment to accurately document how security controls are implemented, and the IT Contingency Plan

for Summit Station is due for an annual test. IT Contingency Plan tests occur every other year to ensure that staff are prepared to handle unexpected IT outages.

Updates to the System Security Plan

In addition to testing the IT Contingency Plan, deployment activities will include an update to all Greenland sections of the Arctic General Support System (GSS) System Security Plan (SSP). SSPs act as a blueprint for IT staff so that the inner workings of a station, system, or process are not limited to specific personnel and can be repeated by other staff or audited by outside entities. Maintaining detailed system security plans is a baseline requirement for a healthy Information Security program and is an IT best practice that ensures the ARC program is compliant with federal standards for information security.

ARC IT Spotlight: Jeffrey Casper, SRI IT & Communications Manager

The Arctic team is full of intelligent, talented, and interesting people; and the team's most recent acquisition is no exception. For this month's IT Spotlight, I sat down with the latest addition to the IT team, SRI IT and Communications Manager, Jeffrey Casper.

Q: You are fairly new to the program, what is the most interesting thing you've learned so far?

A: The first is that in order to provide the proper IT and communications technologies for the researchers, my team receives summaries of their scientific projects. These are in different science fields than my physics background and I enjoy reading the summary of these experiments. I am amazed at the dedication of the researchers to spend so much time in such remote and extreme environments. The second interesting thing comes when you realize that technologies we take for granted on a daily basis are not available at the highest latitudes: GPS is degraded; geostationary satellites are not within line of sight; and polar satellite communications have extremely limited bandwidth.

Q: What do you most look forward to doing as part of the Arctic team?

A: I love developing innovative solutions to hard problems. Some of our tasks for the Arctic team are simple and routine, such as providing satellite phones and personal locator beacons to the researchers. While we never take these for granted as the safety of the researchers is paramount, it's the opportunity to develop and apply new technologies that excites me. The work we are



doing to track the location of researchers, to remotely monitor the status of weather stations and power generators, and to implement a store-and-forward system that lets the researcher to get his data quickly to a relay site where it then trickles back over the available satellite link is the exciting part of the job.

Q: How did you come to support the ARC program?

A: Early in my career at SRI International, I was a Principal Investigator in infrared physics, atmospheric transmission, and atmospheric effects. Having an interest in GPS technology, in the 1990s I worked on the first digitization of the battlespace and became an expert on the employment of commercial technologies for specialized and military applications. My experience in project management along with my background in GPS, communications, and information assurance serves as an ideal background for my current responsibilities in support of the ARC program.